特 許 協 力 条 約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号 P30917-P0	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０３／０７５４１	国際出願日（日.月.年） 13.06.2003	優先日（日.月.年） 14.06.2002
国際特許分類（ＩＰＣ） Int.Cl.[7] G06F12/14, G06F1/00		
出願人（氏名又は名称） 松下電器産業株式会社		

1．この報告書は、ＰＣＴ３５条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

2．この国際予備審査報告は、この表紙を含めて全部で 6 ページからなる。

3．この報告には次の附属物件も添付されている。
a [X] 附属書類は全部で 34 ページである。

[X] 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第６０７号参照）

[X] 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b [ ] 電子媒体は全部で ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。（実施細則第８０２号参照）

4．この国際予備審査報告は、次の内容を含む。

[X] 第Ｉ欄 国際予備審査報告の基礎
[ ] 第Ⅱ欄 優先権
[ ] 第Ⅲ欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
[X] 第Ⅳ欄 発明の単一性の欠如
[X] 第Ⅴ欄 ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
[ ] 第Ⅵ欄 ある種の引用文献
[ ] 第Ⅶ欄 国際出願の不備
[X] 第Ⅷ欄 国際出願に対する意見

国際予備審査の請求書を受理した日 08.04.2004	国際予備審査報告を作成した日 20.12.2004	
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 高橋 克 電話番号 ０３－３５８１－１１０１ 内線 ３５８５	5Ｎ ３０４４

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００４年１月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／０７５４１

第Ⅰ欄　報告の基礎

1．この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

☐ この報告は、＿＿＿＿＿＿ 語による翻訳文を基礎とした。
それは、次の目的で提出された翻訳文の言語である。
☐ ＰＣＴ規則12.3及び23.1(b)にいう国際調査
☐ ＰＣＴ規則12.4にいう国際公開
☐ ＰＣＴ規則55.2又は55.3にいう国際予備審査

2．この報告は下記の出願書類を基礎とした。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☒ 明細書
第 1-3, 5-38 ページ、 出願時に提出されたもの
第 4, 4/1 ページ*、 21.09.2004 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 請求の範囲
第 1-6, 8-13, 15-19, 22-28, 30, 33-39 項、 出願時に提出されたもの
第 ＿＿＿＿ 項*、 ＰＣＴ１９条の規定に基づき補正されたもの
第 14 項*、 08.04.2004 付けで国際予備審査機関が受理したもの
第 7 項*、 21.09.2004 付けで国際予備審査機関が受理したもの

☒ 図面
第 1/12-12/12 ページ~~/図~~、 出願時に提出されたもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

3．☒ 補正により、下記の書類が削除された。

☒ 明細書　第 9/1, 12/1 ページ
☒ 請求の範囲　第 20, 21, 29, 31, 32, 40 項
☐ 図面　第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）
☐ 配列表に関連するテーブル（具体的に記載すること）

4．☒ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

☒ 明細書　第 9-11, 11/1, 12-15 ページ
☒ 請求の範囲　第 19, 22-24, 28, 30, 33-35, 39 項
☐ 図面　第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）
☐ 配列表に関連するテーブル（具体的に記載すること）

＊ 4．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／０７５４１

第Ⅳ欄　発明の単一性の欠如

1．　請求の範囲の減縮又は追加手数料の納付の求めに対して、出願人は、

☐ 請求の範囲を減縮した。

☐ 追加手数料を納付した。

☐ 追加手数料の納付と共に異議を申立てた。

☐ 請求の範囲の減縮も、追加手数料の納付もしなかった。

2．☐ 国際予備審査機関は、次の理由により発明の単一性の要件を満たしていないと判断したが、ＰＣＴ規則68.1の規定に従い、請求の範囲の減縮及び追加手数料の納付を出願人に求めないこととした。

3．　国際予備審査機関は、ＰＣＴ規則13.1、13.2及び13.3に規定する発明の単一性を次のように判断する。

☐ 満足する。

☒ 以下の理由により満足しない。

請求の範囲１は、プログラムを書き換える際に、プログラムを第２の格納手段の外部読出し可能領域に格納し、正当性を判定し、その後、プログラムを第２の格納手段の外部読出し不可能領域に格納する技術に関するものである。

請求の範囲２－４は、プログラムの書き換え後に、プログラムの特定部分のみを読み出す技術に関するものである。

請求の範囲５及び６は、プログラムの書き換え後に、プログラムの一部を実行する技術に関するものである。

請求の範囲７－１４，１６，１７，２８及び３９は、プログラムを書き換える際に、プログラムの正当性を判定する技術に関するものである。

請求の範囲１５及び１８は、発明を特定するための事項が選択肢で表現されており、その選択肢同士が類似の機能を有しない。よって、単一の一般的発明概念を形成しているとはいえない。

請求の範囲１９及び３０は、データを外部からアクセス可能な領域に記憶し、データを外部に出力し、正しく記憶されたか否かを判定し、正しく記憶されたと判定された場合は、データを外部からアクセス不可能な領域に記憶する技術に関するものである。

請求の範囲２２－２７及び３３－３８は、外部からアクセス不可能な領域に記憶されているプログラムの実行結果のみを外部に出力する技術に関するものである。

4．　したがって、国際出願の次の部分について、この報告を作成した。

☒ すべての部分

☐ 請求の範囲 _____ に関する部分

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／０７５４１

第Ｖ欄　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（N）	請求の範囲	1, 15-19, 22-28, 30, 33-39	有
	請求の範囲	2-14	無
進歩性（ＩＳ）	請求の範囲	I	有
	請求の範囲	2-19, 22-28, 30, 33-39	無
産業上の利用可能性（ＩＡ）	請求の範囲	1-19, 22-28, 30, 33-39	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：JP 5-66937 A（沖電気工業株式会社）
1993.03.19，全頁，全図（ファミリーなし）
文献２：JP 63-240629 A
（ニクスドルフ・コンピュータ・アクチエンゲゼルシヤフト）
1988.10.06，全頁，全図 & EP 280035 A2 & US 5224160 A
文献３：JP 62-67800 A（株式会社日立製作所）1987.03.27，全頁，全図
& EP 215464 A2 & US 4777586 A & US 4905142 A

請求の範囲１に記載された発明は、国際調査報告で引用された文献に対して新規性、進歩性を有する。文献には「プログラムを第２の格納手段の外部読出し可能領域に格納し、正当性を判定し、その後、プログラムを第２の格納手段の外部読出し不可能領域に格納すること」が記載されておらず、しかもその点は「プログラムを外部読出し可能領域に格納し、正当性を判定し、その後、プログラムを外部読出し不可能領域に格納すること」から当業者といえども容易に想到し得ないものである。

請求の範囲２－１４に記載された発明は、国際調査報告で引用された文献１により新規性、進歩性を有さない。
文献１には、プログラムを記憶する記憶手段と、演算処理手段と、保存手段とを備えたデータ処理装置において、プログラムの変更部分を保存手段に保存し、正当性を判断した後、記憶手段に記憶する発明が記載されている。
文献１に記載された発明において、プログラムの変更部分が記憶手段に記憶された後、プログラムの変更部分を読出し、実行することは明らかである。

請求の範囲１５－１８に記載された発明は、文献１と、国際調査報告で引用された文献２により、進歩性を有さない。
文献２にはプログラムを暗号化し、検査暗号と比較することにより、プログラムの保全性を確認する発明が記載されている。
文献１に記載された発明における正当性判断方法として、文献２に記載された発明を採用することは、当業者であれば容易に想到し得たものである。

請求の範囲１９，２２－２８，３０，３３－３９に記載された発明は、文献１及び２と、国際調査報告で引用された文献３により、進歩性を有さない。
文献３に記載されているように、プログラムの外部への出力を禁止する技術は周知に過ぎない。
文献１に記載されている発明においても、外部への出力を禁止した記憶手段にプログラムを記憶することは、当業者であれば容易に想到し得たものである。

第Ⅷ欄　国際出願に対する意見

請求の範囲、明細書及び図面の明瞭性又は請求の範囲の明細書による十分な裏付についての意見を次に示す。

１．請求の範囲の明瞭性について
（１）請求の範囲１，１９，２２－２４，２８，３０，３３－３５及び３９について
請求の範囲１，１９，２２－２４，２８，３０，３３－３５及び３９に記載された「外部読み出し可能領域」、「外部読み出し不可領域」、「外部からアクセス可能な領域」及び「外部からアクセス不可能な領域」という事項は明瞭でない。
これらの記載は、請求の範囲に係る発明を機能で特定しようとするものであるが、これらの記載のみから、発明の具体的な構成を想定することはできない。

２．明細書による裏付けについて
（１）請求の範囲１，１９，２２－２４，２８，３０，３３－３５及び３９について
請求の範囲１，１９，２２－２４，２８，３０，３３－３５及び３９は、明細書によって十分に裏付けされていない。
明細書には、「外部からのアドレスバスは外部読出し可能領域と同様外部読出し不可能領域に接続するが、外部にデータを読み出す場合はデータバスは外部読出し不可能領域には接続しないスイッチを設けることで実現できる」ことが記載されているものの、この方法以外に「外部読み出し可能領域」、「外部読み出し不可領域」、「外部からアクセス可能な領域」及び「外部からアクセス不可能な領域」という領域を実現する具体的な方法は一切開示されていない。また、明細書に記載された内容を「外部読み出し可能領域」、「外部読み出し不可領域」、「外部からアクセス可能な領域」及び「外部からアクセス不可能な領域」といった事項の範囲まで上位概念化できるともいえない。

（２）請求の範囲５及び６について
請求の範囲５及び６は、明細書によって十分に裏付けされていない。明細書には、プログラムの機密性を保ちながら、該書き換えプログラムが半導体集積回路内の書き換え可能なＲＡＭに正しく格納されているかを確認するために、プログラムを格納した後、プログラムの一部を実行し、正しく実行できたか否かを判断することが記載されている。しかしながら、請求項５及び６には、プログラムを実行することが記載されているものの、正しく実行できたか否かを判断する構成が反映されていない。

補充欄

いずれかの欄の大きさが足りない場合

第　I　欄の続き

出願時における開示の範囲を超えてなされた補正について

補正された明細書第９－１１，１１／１及び１２－１５頁と、請求の範囲１９，２２－２４，２８，３０，３３－３５及び３９項は、出願時における開示の範囲を超えている。

「データを外部からアクセス可能な領域に記憶させる」という事項を「データを外部からアクセス可能な領域を有する記憶手段に記憶させる」という事項に補正することは、出願時における明細書に記載されていない事項を追加することになる。

また、本発明の請求の範囲第１８項に記載の半導体集積回路装置は、請求の範囲第１項ないし第１７項のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたものである。

これにより、書き換えプログラムを半導体集積回路装置外部に有する場合においても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる。

また、本発明の請求の範囲第１９項に記載のデータ記憶検証装置は、任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる手段と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する手段と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段とを備えた、ことを特徴とするものである。

これにより、例えばダミーデータなどを、上記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく上記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２０項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、前記機密データの特定部分を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データの特定部分のみを読み出して、該特定部分を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２１項に記載のデータ記憶検証装置は、プログラムを含んだ機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、前記記憶されたプログラムを実行させ、結果を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれ

ているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２２項に記載のデータ記憶検証装置は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の手段と、前記検査プログラムを実行させ、結果を外部に出力する第２の手段と、前記第２の手段の終了後、前記機密プログラムを実行させる第３の手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

また、本発明の請求の範囲第２３項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、前記演算の結果を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２４項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な第１の領域を有する記憶手段に記憶させる第４の手段と、機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域を有する記憶手段に記憶させる第５の手段と、前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の手段とを備えた、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な第１の領域に格納するとともに、その機密データの一部である検査プログラムを第２の領域に格納し、この検査プログラムを用いて検査を行い、その検査結果を外部に出力して、第１の

領域の機密データの正当性を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２５項に記載のデータ記憶検証装置は、請求項２４記載のデータ記憶検証装置において、前記第６の手段の終了後に前記第１の領域の命令に制御を移す第７の手段をさらに備えた、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認した後に、本来の機密データに含まれる命令の実行に移ることができる。

また、本発明の請求の範囲第２６項に記載のデータ記憶検証装置は、請求項２４記載のデータ記憶検証装置において、前記第５の手段は、前記第１の領域に記憶されている機密データ内に存在する命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データ内に存在する命令により行うことができる。

また、本発明の請求の範囲第２７項に記載のデータ記憶検証装置は、請求項２４記載のデータ記憶検証装置において、前記第５の手段は、第３の領域に前記第４の手段による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データを格納するより前に格納した命令により行うことができる。

また、本発明の請求の範囲第２８項に記載のデータ記憶検証装置は、機密データを復号する手段と、前記復号されたデータを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、前記記憶されたデータを暗号化する手段と、前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する手段とを備えた、ことを特徴とするものである。

これにより、いったん復号して外部からアクセス不可能な領域に格納した機密

データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２９項に記載のデータ記憶検証装置は、機密プログラムを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、前記記憶されたプログラムを読み出す手段と、前記読み出されたプログラムを命令単位で正当性を判定する手段と、正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域を有する記憶手段において空いている領域に記憶させる手段と、前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる手段と、正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる手段とを備えた、ことを特徴とするものである。

これにより、機密プログラムを外部からアクセス不可能な領域に格納し、その格納したプログラムを読み出し命令単位で正当性を判定し、正当でないと判定された命令に対しては外部からアクセス不可能な領域の空き領域に格納した正当な命令にジャンプすることにより、機密プログラムを格納する際にその一部に正しく格納できていない命令が含まれていても、空き領域に格納した正しい命令に置換してこれを実行することができる。

また、本発明の請求の範囲第３０項に記載のデータ記憶検証方法は、任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる工程と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程とを含む、ことを特徴とするものである。

これにより、例えばダミーデータなどを、前記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく前記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３１項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、前記

機密データの特定

部分を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データの特定部分のみを読み出して、該特定部分を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３２項に記載のデータ記憶検証方法は、プログラムを含んだ機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、前記記憶されたプログラムを実行させ、結果を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３３項に記載のデータ記憶検証方法は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の工程と、前記検査プログラムを実行させ、結果を外部に出力する第２の工程と、前記第２の工程の終了後、前記機密プログラムを実行させる第３の工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

また、本発明の請求の範囲第３４項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、前記演算の結果を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、前記機密データが正しくダウンロードできたか

否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３５項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な第１の領域を有する記憶手段に記憶させる第４の工程と、機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域を有する記憶手段に記憶させる第５の工程と、前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の工程とを含む、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な第１の領域に格納するとともに、その機密データの一部である検査プログラムを第２の領域に格納し、この検査プログラムを用いて検査を行い、その検査結果を外部に出力して、第１の領域の機密データの正当性を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３６項に記載のデータ記憶検証方法は、請求項３５記載のデータ記憶検証方法において、前記第６の工程の終了後に前記第１の領域の命令に制御を移す第７の工程をさらに含む、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認した後に、本来の機密データに含まれる命令の実行に移ることができる。

また、本発明の請求の範囲第３７項に記載のデータ記憶検証方法は、請求項３５記載のデータ記憶検証方法において、前記第５の工程は、前記第１の領域に記憶されている機密データ内に存在する命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データ内に存在する命令により行うことができる。

また、本発明の請求の範囲第３８項に記載のデータ記憶検証方法は、請求項３５記載のデータ記憶検証方法において、前記第５の工程は、前記第３の領域に前記第４の工程による記憶の実行以前に記憶された命令により前記検査プログラム

の記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データを格納するより前に格納した命令により行うことができる。

また、本発明の請求の範囲第３９項に記載のデータ記憶検証方法は、機密データを復号する工程と、前記復号されたデータを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、前記記憶されたデータを暗号化する工程と、前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する工程とを含む、ことを特徴とするものである。

これにより、いったん復号して外部からアクセス不可能な領域に格納した機密データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第４０項に記載のデータ記憶検証方法は、機密プログラムを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、前記記憶されたプログラムを読み出す工程と、前記読み出されたプログラムを命令単位で正当性を判定する工程と、正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域を有する記憶手段において空いている領域に記憶させる工程と、前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる工程と、正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる工程とを含む、ことを特徴とするものである。

これにより、機密プログラムを外部からアクセス不可能な領域に格納し、その格納したプログラムを読み出し命令単位で正当性を判定し、正当でないと判定された命令に対しては外部からアクセス不可能な領域の空き領域に格納した正当な命令にジャンプすることにより、機密プログラムを格納する際にその一部に正しく格納できていない命令が含まれていても、空き領域に格納した正しい命令に置換してこれを実行することができる。

前回の判定結果が正しいと判定されたときに、前回２分割した領域の一方の領域を、プログラムが格納されていない領域としてさらに２分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、

上記第２の格納手段に格納すべきプログラムすべてを順次格納する、

ことを特徴とする半導体集積回路装置。

１２．　請求の範囲第１１項に記載の半導体集積回路装置において、

上記第２の格納手段は、該第２の格納手段の上記書き換えプログラムが格納されていない領域を順次２分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとした、

ことを特徴とする半導体集積回路装置。

１３．　請求の範囲第１２項に記載の半導体集積回路装置において、

上記一意に得られるデータが、該プログラムデータの反転データである、

ことを特徴とする半導体集積回路装置。

１４．（補正後）　請求の範囲第８項ないし第１３項のいずれかに記載の半導体集積回路装置において、

上記チェックプログラムを予め格納したＲＯＭ(Read Only Memory)を備え、

上記ＲＯＭにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行う、

ことを特徴とした半導体集積回路装置。

１５．　請求の範囲第１項ないし第１４項のいずれかに記載の半導体集積回路装置において、

上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、

上記第１の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第２の格納手段に復号化した上記書き換えプログラムを格納する、

ことを特徴とする半導体集積回路装置。

１６．　半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさ

せるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第１の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第２の格納手段に転送する復号化手段と、

上記第２の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、

上記暗号化手段で暗号化された書き換えプログラムと上記第１の格納手段に保持している暗号化された書き換えプログラムとを比較する、

ことを特徴とする半導体集積回路装置。

１７．　請求の範囲第１１項ないし第１３項、及び第１６項のいずれかに記載の半導体集積回路装置において、

上記第２の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第１の格納手段に保持した書き換えプログラムを修正可能とした、

ことを特徴とする半導体集積回路装置。

１８．　請求の範囲第１項ないし第１７項のいずれかに記載の半導体集積回路装置において、

当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能とした、

ことを特徴とする半導体集積回路装置。

１９．（補正後）　任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる手段と、

前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する手段と、

正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２０．（補正後） 機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、

前記機密データの特定部分を外部に出力する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２１．（補正後） プログラムを含んだ機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、

前記記憶されたプログラムを実行させ、結果を外部に出力する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２２．（補正後） 検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の手段と、

前記検査プログラムを実行させ、結果を外部に出力する第２の手段と、

前記第２の手段の終了後、前記機密プログラムを実行させる第３の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２３．（補正後） 機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、

前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、

前記演算の結果を外部に出力する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２４．（補正後） 機密データを外部からアクセス不可能な第１の領域を有する記憶手段に記憶させる第４の手段と、

機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域を有する記憶手段に記憶させる第５の手段と、

前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２５． 請求項２４記載のデータ記憶検証装置において、

前記第６の手段の終了後に前記第１の領域の命令に制御を移す第７の手段をさらに備えた、

ことを特徴とするデータ記憶検証装置。

２６． 請求項２４記載のデータ記憶検証装置において、

前記第５の手段は、前記第１の領域に記憶されている機密データ内に存在する

命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

２７．　請求項２４記載のデータ記憶検証装置において、

前記第５の手段は、第３の領域に前記第４の手段による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

２８．（補正後）　機密データを復号する手段と、

前記復号されたデータを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、

前記記憶されたデータを暗号化する手段と、

前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２９．（補正後）　機密プログラムを外部からアクセス不可能な領域を有する記憶手段に記憶させる第２１の手段と、

前記記憶されたプログラムを読み出す第２２の手段と、

前記読み出されたプログラムを命令単位で正当性を判定する第２３の手段と、

正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域を有する記憶手段において空いている領域に記憶させる第２４の手段と、

前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる第２５の手段と、

正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる第２６の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

３０．（補正後）　任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる工程と、

前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、

正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程とを含む、

ことを特徴とするデータ記憶検証方法。

３１．（補正後） 機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、

前記機密データの特定部分を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

３２．（補正後） プログラムを含んだ機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、

前記記憶されたプログラムを実行させ、結果を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

３３．（補正後） 検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の工程と、

前記検査プログラムを実行させ、結果を外部に出力する第２の工程と、

前記第２の工程の終了後、前記機密プログラムを実行させる第３の工程とを含む、

ことを特徴とするデータ記憶検証方法。

３４．（補正後） 機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、

前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、

前記演算の結果を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

３５．（補正後） 機密データを外部からアクセス不可能な第１の領域を有する記憶手段に記憶させる第４の工程と、

機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域を有する記憶手段に記憶させる第５の工程と、

前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の工程とを含む、

ことを特徴とするデータ記憶検証方法。

３６． 請求項３６記載のデータ記憶検証方法において、

前記第６の工程の終了後に前記第１の領域の命令に制御を移す第７の工程をさらに含む、

ことを特徴とするデータ記憶検証方法。

３７． 請求項３５記載のデータ記憶検証方法において、

前記第５の工程は、前記第１の領域に記憶されている機密データ内に存在する

命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

３８．　請求項３５記載のデータ記憶検証方法において、

前記第５の工程は、前記第３の領域に前記第４の工程による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

３９．（補正後）　機密データを復号する工程と、

前記復号されたデータを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、

前記記憶されたデータを暗号化する工程と、

前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する工程とを含む、

ことを特徴とするデータ記憶検証方法。

４０．（補正後）　機密プログラムを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、

前記記憶されたプログラムを読み出す工程と、

前記読み出されたプログラムを命令単位で正当性を判定する工程と、

正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域を有する記憶手段において空いている領域に記憶させる工程と、

前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる工程と、

正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる工程とを含む、

ことを特徴とするデータ記憶検証方法。

に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第５項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、上記第２の格納手段に格納した上記書き換えプログラムの一部を実行するものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第６項に記載の半導体集積回路装置は、請求の範囲第５項に記載の半導体集積回路装置において、上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである。

これにより、例えば、上記第２の格納手段に格納された上記書き換えプログラムの先頭プログラムと最終プログラムとを実行した場合、該書き換えプログラムが最後まで正しく格納できたかを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第７項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第１の格納手段から上記第２の格納手段に転送される上記書き換えプログラムの転送エラーを監視する転送監視手段を備え

たものである。

また、本発明の請求の範囲第１８項に記載の半導体集積回路装置は、請求の範囲第１項ないし第１７項のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたものである。

これにより、書き換えプログラムを半導体集積回路装置外部に有する場合においても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる。

また、本発明の請求の範囲第１９項に記載のデータ記憶検証装置は、任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる手段と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する手段と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段とを備えた、ことを特徴とするものである。

これにより、例えばダミーデータなどを、上記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく上記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２２項に記載のデータ記憶検証装置は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の手段と、前記検査プログラムを実行させ、結果を外部に出力する第２の手段と、前記第２の手段の終了後、前記機密プログラムを実行させる第３の手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

また、本発明の請求の範囲第２３項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、前記演算の結果を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２４項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な第１の領域を有する記憶手段に記憶させる第４の手段と、機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域を有する記憶手段に記憶させる第５の手段と、前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の手段とを備えた、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な第１の領域に格納するとともに、その機密データの一部である検査プログラムを第２の領域に格納し、この検査プログラムを用いて検査を行い、その検査結果を外部に出力して、第１の

データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３０項に記載のデータ記憶検証方法は、任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる工程と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる工程とを含む、ことを特徴とするものである。

これにより、例えばダミーデータなどを、前記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく前記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３３項に記載のデータ記憶検証方法は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の工程と、前記検査プログラムを実行させ、結果を外部に出力する第２の工程と、前記第２の工程の終了後、前記機密プログラムを実行させる第３の工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

また、本発明の請求の範囲第３４項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、前記演算の結果を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、前記機密データが正しくダウンロードできたか

の記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データを格納するより前に格納した命令により行うことができる。

また、本発明の請求の範囲第３９項に記載のデータ記憶検証方法は、機密データを復号する工程と、前記復号されたデータを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、前記記憶されたデータを暗号化する工程と、前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する工程とを含む、ことを特徴とするものである。

これにより、いったん復号して外部からアクセス不可能な領域に格納した機密データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

4． 請求の範囲第２項に記載の半導体集積回路装置において、

上記制御回路は、上記第２の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとした、

ことを特徴とする半導体集積回路装置。

5． 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、

上記第２の格納手段に格納した上記書き換えプログラムの一部を実行する、

ことを特徴とする半導体集積回路装置。

6． 請求の範囲第５項に記載の半導体集積回路装置において、

上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである、

ことを特徴とする半導体集積回路装置。

7．（補正後） 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第１の格納手段から上記第２の格納手段に転送される上記書き換えプログラムの転送エラーを監視する転送監視手段を備えた、

ことを特徴とする半導体集積回路装置。

8． 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回

20.（削除）

21．（削除）

22．　検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の手段と、

前記検査プログラムを実行させ、結果を外部に出力する第２の手段と、

前記第２の手段の終了後、前記機密プログラムを実行させる第３の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

23．　機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、

前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、

前記演算の結果を外部に出力する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

24．　機密データを外部からアクセス不可能な第１の領域を有する記憶手段に記憶させる第４の手段と、

機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域を有する記憶手段に記憶させる第５の手段と、

前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

25．　請求項２４記載のデータ記憶検証装置において、

前記第６の手段の終了後に前記第１の領域の命令に制御を移す第７の手段をさらに備えた、

ことを特徴とするデータ記憶検証装置。

26．　請求項２４記載のデータ記憶検証装置において、

命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

２７．　請求項２４記載のデータ記憶検証装置において、

前記第５の手段は、第３の領域に前記第４の手段による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

２８．　機密データを復号する手段と、

前記復号されたデータを外部からアクセス不可能な領域を有する記憶手段に記憶させる手段と、

前記記憶されたデータを暗号化する手段と、

前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２９．（削除）

３０．　任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる工程と、

前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、

正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程とを含む、

ことを特徴とするデータ記憶検証方法。

３１．（削除）

３２．（削除）

３３．　検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる第１の工程と、

前記検査プログラムを実行させ、結果を外部に出力する第２の工程と、

前記第２の工程の終了後、前記機密プログラムを実行させる第３の工程とを含む、

ことを特徴とするデータ記憶検証方法。

３４．　機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、

前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、

前記演算の結果を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

３５．　機密データを外部からアクセス不可能な第１の領域を有する記憶手段に記憶させる第４の工程と、

機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域を有する記憶手段に記憶させる第５の工程と、

前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の工程とを含む、

ことを特徴とするデータ記憶検証方法。

３６．　請求項３６記載のデータ記憶検証方法において、

前記第６の工程の終了後に前記第１の領域の命令に制御を移す第７の工程をさらに含む、

ことを特徴とするデータ記憶検証方法。

３７．　請求項３５記載のデータ記憶検証方法において、

命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

３８．　請求項３５記載のデータ記憶検証方法において、

前記第５の工程は、前記第３の領域に前記第４の工程による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

３９．　機密データを復号する工程と、

前記復号されたデータを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程と、

前記記憶されたデータを暗号化する工程と、

前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する工程とを含む、

ことを特徴とするデータ記憶検証方法。

４０．（削除）

データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３０項に記載のデータ記憶検証方法は、任意のデータを外部からアクセス可能な領域を有する記憶手段に記憶させる工程と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域を有する記憶手段に記憶させる工程とを含む、ことを特徴とするものである。

これにより、例えばダミーデータなどを、前記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく前記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。